UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION AT DAYTON

UNITED STATES OF AMERICA,

Plaintiff,

Case No. 3:14-cr-023

-vs-

Judge Thomas M. Rose

DEMIAN PINA,

Defendant.

Entry and Order Denying Motion to Suppress Evidence, Doc. 34 and Granting Motion *in Limine* for a Ruling as to the Authentication of Domestic Records of Regularly Conducted Activity. Doc. 51.

This matter comes before the Court pursuant to Defendant's Motion to Suppress Evidence, Doc. 34, and the Government's Motion *in Limine* for a Ruling as to the Authentication of Domestic Records of Regularly Conducted Activity. Doc. 51. Because the Government's search warrant application was supported by probable cause and was executed in good faith, Defendant's motion will be denied. Because a written declaration attesting to the authenticity of a business record has been ruled non-testimonial in nature, excluding it from the reach of *Crawford v. Washington*, 584 U.S. 36 (2004), the Government's motion will be granted.

Defendant Demian Pina was indicted on February 25, 2014, on five counts of distribution of child pornography and two counts of possession of child pornography. These charges stemmed from the execution of two search warrants on separate occasions at Pina's residence.

In late 2010, investigators from the Cuyahoga County Internet Crimes Against Children Task Force conducted an online Internet investigation to identify individuals possessing and sharing child

pornography. On November 30, 2010, while working in an undercover capacity, an investigator identified a computer with an IP address of 64.56.112.147 sharing approximately 447 files, at least 7% of which contained file names or hash values known to relate to child pornography. Between approximately 8:30 a.m. and 8:33 a.m. on November 30, 2010, the investigator utilized a law enforcement tool that allowed single-source downloads to select and download eight image files and four video files from the shared files of the suspect computer. One file is named in part "Steve 01." This file is alleged to contain a video of oral sexual activity involving two pre-pubescent white male children.

The investigator requested and received records pursuant to an administrative subpoena relating to the identified IP address, which identified the subscriber as Demian Pina giving his address in Dayton, Ohio, during the date and times that the investigator downloaded files containing child pornography from this IP address. This information was turned over to the Federal Bureau of Investigation, Dayton Field Office.

On February 10, 2011, United States Magistrate Judge Sharon L. Ovington, authorized a search warrant for Pina's residence for evidence of receipt and possession of child pornography. FBI agents and officers of the Dayton Police Department executed the search warrant on February 11, 2011. In the warrant application, the agents and officers had identified that Demian Pina resided at the residence along with his mother. Pursuant to the warrant, agents seized computer equipment.

During the execution of the search warrant, Pina consented to be interviewed. Pina stated that all of the computers in the residence belonged to him. He also said he received training in computers while in the Army. Pina declined to answer questions related to searching for and viewing

child pornography.

The Dayton Police Department submitted all seized electronic media to the Miami Valley Regional Computer Forensic Laboratory for analysis. An examiner trained in identifying child pornography reviewed the media. The examination confirmed the presence of child pornography on the computers belonging to Pina, as well as a file sharing program that had been utilized by the undercover officers during their investigation.

The second search Pina contests occurred in late 2012. In November 2012, investigators from the Cuyahoga County Internet Crimes Against Children Task Force were again conducting online Internet investigations to identify individuals possessing and sharing child pornography. On November 29, 2012, an undercover investigator identified that a computer with an IP address of 108.253.71.47 was sharing approximately 170 files, 18% of which contained file names or hash values consistent with child pornography. Between approximately 6:12 p.m. and 6:19 p.m. on November 29, 2012, the investigator downloaded five image files from the shared files of the computer with an IP address 108.253.71.47. One of the files is named in part "boys in action." This file is alleged to contain image of a pre-pubescent white male child, nude from the waist down, being raped.

The investigator determined that the IP address was serviced by AT&T Internet Services. Records received pursuant to an administrative subpoena identified that this IP address resolved to Pina's address during the date and times when the investigator downloaded files containing child pornography. The subscriber name associated with the account was identified as Pina's mother. The records indicated that the account had been active since July 25, 2012.

Later, in March and April 2013, a detective with the Troy, Ohio Police Department conducted

an online Internet investigation to identify individuals possessing and sharing child pornography. On March 15, 2013, while working undercover, a detective identified that a computer with an IP address of 108.253.71.47 was sharing approximately 35 files, approximately four of which contained file names or hash values known to contain child pornography. Between approximately 3:46 p.m. and 3:51 p.m. on March 15, 2013, the detective downloaded four image files from the shared files of the computer with an IP address 108.253.71.47. One of the files was another file named in part "Boys in Action [2]," allegedly containing images of three pre-pubescent boys engaged in sexual activity. On March 17 and 19, 2013, the same detective downloaded two more images of pre-pubescent white males engaged in sexual activity.

Similar to the above investigations, the detective determined the IP address of 108.253.71.47 was serviced by AT&T Internet Services. The detective also received records pursuant to an administrative subpoena, which determined that this IP address was subscribed to Pina's mother at the same address as before, since July 25, 2012. All of the information referencing the 2012 and 2013 downloads by undercover investigators was turned over to the FBI, Dayton Field Office.

On June 3, 2013, United States Magistrate Judge Michael J. Newman authorized the second search warrant for Pina's residence. Agents with the FBI and officers of the Dayton Police Department executed this search warrant on June 4, 2013. Agents and officers identified that Pina and his mother still resided at the residence. They seized computers, external hard drives, and other computer equipment.

Pina's mother stated that her son repaired computers as a source of income, and that some of the computers in the residence belonged to others. Because of Pina's refusal to comply with safety

commands, he was placed in handcuffs shortly after agents entered his residence. He was instructed he was free to leave the residence or remain. He chose to remain, but refused to stay in a single location. Because of this, the officers placed him in handcuffs. The officers read Pina his rights and Pina acknowledged he understood them.

Electronic media seized pursuant to the search warrant were submitted to the Miami Valley Regional Computer Forensic Laboratory and an examiner trained in identifying child pornography reviewed the media. The examination confirmed the presence of child pornography on computer items connected to Pina.

Pina contends, "An individual's reasonable expectations of privacy should not be subject to arbitrary invasions solely at the unfettered discretion of officers in the field" Doc. 34 at 1, PAGEID 93, (citing *Brown v. Texas*, 443 U.S. 47, 51 (1979)). As stated more fully in the *Brown* decision:

> A central concern in balancing these competing considerations in a variety of settings has been to assure that an individual's reasonable expectation of privacy is not subject to arbitrary invasions solely at the unfettered discretion of officers in the field. See *Delaware v. Prouse*, 440 U.S. 648, 654–655, 99 S. Ct. 1391, 1396–1397, 59 L.Ed.2d 660 (1979); *United States v. Brignoni-Ponce*, 422 U.S., at 882, 95, at 2580. To this end, the Fourth Amendment requires that a seizure must be based on specific, objective facts indicating that society's legitimate interests require the seizure of the particular individual, or that the seizure must be carried out pursuant to a plan embodying explicit, neutral limitations on the conduct of individual officers. *Delaware v. Prouse*, 440 U.S at 663, 99 S. Ct., at 1401. See *United States v. Martinez-Fuerte*, 428 U.S. 543, 558–562, 96 S. Ct. 3074, 3083–3085, 49 L.Ed.2d 1116 (1976).

Brown v. Texas, 443 U.S. at 51.

Pina asserts that the warrants lacked sufficient probable cause to be valid and further asserts

that, as a result, all evidence seized including statements Pina made must be suppressed as "fruit of the poisonous tree" pursuant to *Wong Sun v. United States*, 371 U.S. 471, 488, 83 S. Ct., 407, 417, 9 L. Ed. 2nd 441, 455 (1963).

Pina's reasonable expectation of privacy was not subject to an arbitrary invasion solely at the unfettered discretion of officers in the field. The investigating officers arrived at his residence in the execution of search warrants that issued with the support of probable cause.

Probable cause exists "when there is a 'fair probability' ... that contraband or evidence of a crime will be found in a particular place." *United States v. Helton*, 314 F.3d 812, 819 (6th Cir. 2003). It is only necessary that an issuing officer find "reasonable grounds for belief that evidence will be found in order to justify the issuance of a search warrant." *United States v. Bennett*, 905 F.2d 931, 934 (6th Cir. 1990). The "test for probable cause is simply whether 'there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" *United States v. Padro*, 52 F.3d 120, 123 (6th Cir. 1995).

With regard to the 2011 search, the affidavit set forth particular details related to the investigation which established probable cause. The affidavit provided information related to computers and the significance of Internet Protocol (IP) addresses. (See Doc. 48-1, pp. 3-8, PAGEID 196-201). Also, the affidavit set forth "behavioral characteristics" common to those who have a sexual interest in children, particularly how it relates to online activity. (*Id.* pp. 15- 21, PAGEID 211-17). Additionally, the affidavit specifically set forth facts related to how Pina's address had been identified, that a person at Pina's address was suspected of making child pornography available over the internet, and why the agent believed evidence of a crime would be discovered at Pina's residence.

The 2011 affidavit detailed how an undercover agent downloaded child pornography from a particular IP address. That IP address resolved to Pina's residence at the specific date of the downloads. The agent then took further steps to confirm the residence was associated with Pina, by conducting a LexisNexis search of Pina and confirming his driver's license information.

The 2013 affidavit also established probable cause to search Pina's residence. (See Doc. 48-2, PAGEID 231-53). Again, the agent making the application provided general information on computers, common characteristics of collectors of child pornography, and how computers and the internet are used in child pornography. The affidavit described peer-to-peer file sharing programs and how they are used to trade and receive child pornography. The 2013 affidavit then detailed two investigations conducted by different law enforcement agencies, in addition to giving the background of the 2011 search.

In November 2012 an investigator with Cuyahoga County connected to a computer that resolved to Pina's address and downloaded child pornography files. In March and April of 2013 a detective with the Troy Police Department also connected to a computer that resolved to Pina's address and downloaded child pornography files. Both law enforcement officers identified the particular IP addresses used in the downloads and took appropriate steps to confirm subscriber information. That information indicated the IP addresses resolved to Pina's residence. The agent further confirmed the identity of persons residing at the address, which were Pina and his mother. Given this testimony, there was a "fair probability" that the evidence of a crime would be located at Pina's residence in 2011 and in 2013.

In issuing a search warrant or in reviewing the decision to issue one, a judge must apply a

"totality of the circumstances" test to issues of probable cause. *Illinois v. Gates*, 462 U.S. 213, 238 (1983). The totality of the circumstances test requires a "practical common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information," that probable cause exists. *Id.*

In both affidavits, the agents set forth all of the factors which established probable cause to believe evidence of a crime would be found at the identified location. The affidavit identified statutes violated by Pina, or someone residing at his residence. Here, the proper test is whether sufficient information was set forth to conclude that evidence of a crime would be found at the residence searched. There was.

Because the warrants were supported by probable cause there is no basis to suppress statements Pina made as "fruit of the poisonous tree." *Wong Sun v. United States*, 371 U.S. 471 (1963).

In the event that a reviewing court were to find that the search warrants should not have issued, the Government seeks protection in the "good faith" exception enunciated in *United States v. Leon*, 468 U.S. 897 (1984). According to *Leon*, "When evidence is obtained in violation of the Fourth Amendment, the judicially developed exclusionary rule usually precludes its use in a criminal proceeding against the victim of the illegal search and seizure." *Illinois v. Krull*, 480 U.S. 340, 347 (1987). However, courts should not suppress "evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant." *United States v. Leon*, 468 U.S. at 922.

The Sixth Circuit has identified four specific situations in which an officer's reliance on a subsequently invalidated warrant cannot be considered objectively reasonable: (1) when the warrant is

issued on the basis of an affidavit that the affiant either knows to contain false information or recklessly disregards the existence of false information in it; (2) when the issuing magistrate abandons his neutral and detached role and serves as a rubber stamp for police activities; (3) when the affidavit is so lacking in indicia of probable cause that a belief in its existence is objectively unreasonable; and (4) when the warrant is so facially deficient that it cannot be reasonably presumed to be valid. *United States v. Laughton*, 409 F.3d 744, 748 (6th Cir. 2005). The first of the two situations are not at issue in this case.

If the affidavit before the Court failed to establish probable cause, the relevant inquiry would be whether the agents had a reasonable basis to believe that the information submitted supported the issuance of the search warrant. *United States v. Carpenter*, 360 F.3d 591, 595 (6th Cir. 2004). In the matter before the Court, the agents acted in good faith in executing both search warrants.

First, an objective law enforcement officer, after reviewing the affidavits, would have concluded there was a fair probability that evidence of criminal conduct would be found at Pina's residence in 2011 and 2013. The affidavits established that someone at the residence used a computer to facilitate crimes by making child pornography available on a file sharing program. An objective law enforcement officer reviewing the affidavits would have concluded the affidavits were sufficient to establish probable cause in light of the totality of the information contained within the affidavits.

Consistent with *Leon*, evidence "will not be excluded…unless the illegality is at least the 'but for' cause of the discovery of the evidence," unless that is "'the challenged evidence is in some sense the product of illegal governmental activity.'" *United States v. Clariot*, – F.3d. –, 2011 WL 3715235 at

p. 3 (6th Cir. 2011); quoting *Segura v. United States*, 468 U.S. 796, 815 (1984). Here, the exclusionary rule works in favor of the government. Both agents' conduct was not in question. They did not engage in any illegal or impermissible behavior. The purpose of the exclusionary rule is to punish, through the prohibition of evidence, conduct which clearly demonstrates an officer or agent acted in bad faith. In the instant case, this did not occur in the execution of either warrant. Therefore, the evidence in this matter will not be suppressed.

Finally, the Court considers the Government's Motion for a Ruling as to the Authentication of Domestic Records of Regularly Conducted Activity. Doc. 51. At trial, the Government intends to offer in evidence business records provided by internet service providers DONet and AT&T Internet Services. Each of the Internet Service Providers provided to investigators records correlating subscriber information to the internet protocol addresses identified during the investigations. The first set of records was provided by DONet and relates to subscriber information associated with IP address 64.56.112.147 used on November 30, 2010. The second set of business records was provided by AT&T Internet Services and relates to subscriber information associated with IP address 108.253.71.47 used on November 29, 2012. The third, and final, set of records was provided by AT&T Internet Services and relates to IP address 108.253.71.47 used on March 15 and 17, 2013.

The Government informs the Court that the custodians of records for AT&T Internet Services are located in Georgia and Connecticut. According to the Government, Federal Rule of Evidence 902(11) permits authentication of such records by a written declaration of its custodian or other qualified person. Rule 902(11) states:

> Extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to the following:

> (11) Certified Domestic Records of Regularly Conducted Activity.-- The original or a duplicate of a domestic record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any . . . rule prescribed by the Supreme Court pursuant to statutory authority. . .

Fed. R. Evid. 902(11).

Pina contests that the Sixth Amendment of the United States Constitution as construed in *Crawford v. Washington*, 541 U.S. 36 (2004), entitles him to confront those witnesses that would present evidence against him. A written declaration attesting to the authenticity of a business record, however, is not testimonial in nature. The Supreme Court specifically observed that business records "by their nature are not testimonial." *Crawford v. Washington*, 584 U.S. 36, 56 (2004). So long as the government provides sufficient written notice of its intent to use business records and the records are accompanied by a written declaration, they are admissible, subject to other Rules of Evidence. See *United States v. Jordan*, 544 F.3d 656, 669-70 (6th Cir. 2008).

The United States provided Pina with written declarations of authenticity and provided copies of the documents it intends to use at trial. Accordingly, the United States asks for a ruling by this Court in advance of trial allowing authentication of the above described business records by declarations complying with Federal Rule of Evidence 902(11) and 28 U.S.C. §1746, copies of which have been made available or provided to the defense and are attached to this motion.

DONE and ORDERED in Dayton, Ohio on Friday, June 12, 2015.

s/Thomas M. Rose

THOMAS M. ROSE
UNITED STATES DISTRICT JUDGE